STEP3 LAB: RESOURCES AND PROCEDURES NOTES

Resources

1. A Windows system, WINFOR01, with Forensic Toolkit (FTK) Imager installed.
2. A flash drive image file "FlashDrive.img" (Provided).

Virtual Machine Credentials

Username: **StudentFirst**

Password: **Cyb3rl@b**

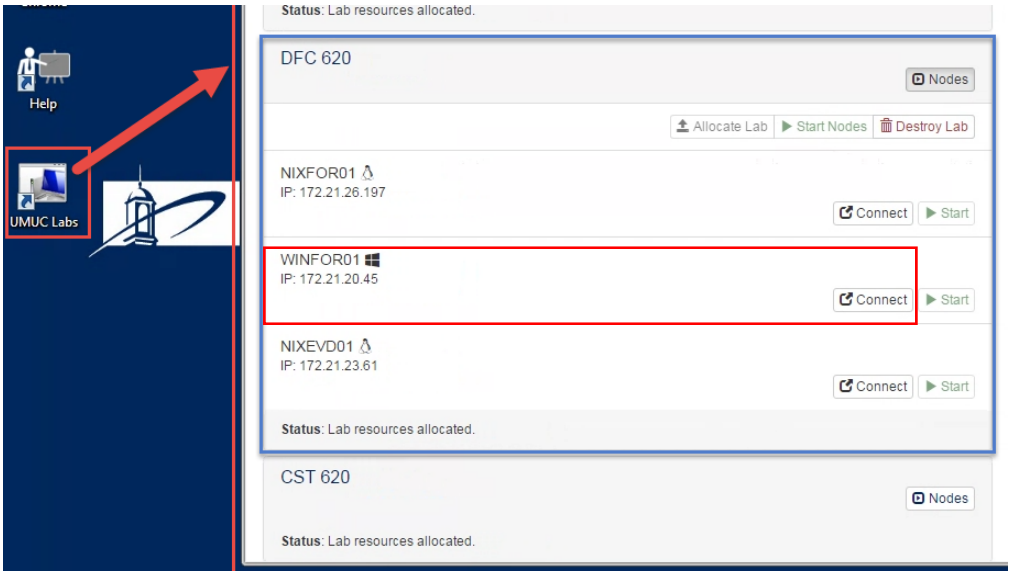
Procedure Notes

1. These procedures assume that your evidence computer is Windows 7 or later
2. Placeholders are in [brackets]
3. Comments are in *(parentheses and italics)*
4. Command line instructions are indicated as follows:

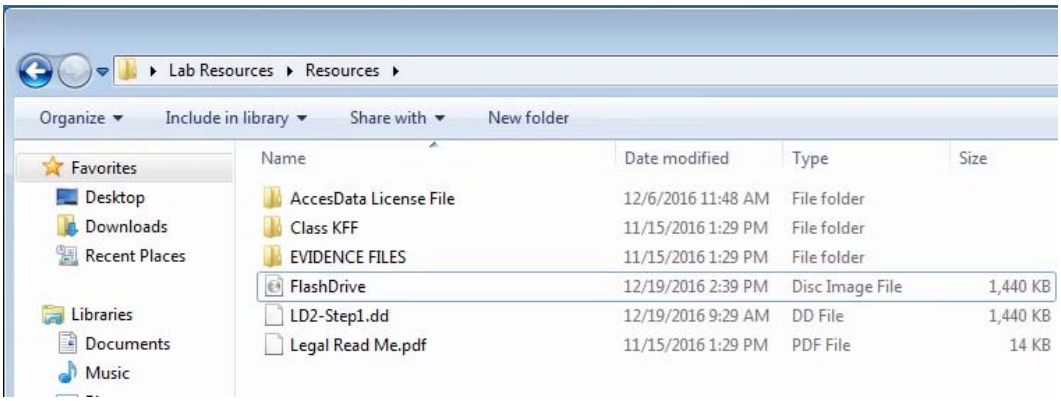
- > command *(Windows normal user)*
- admin> command *(Windows Administrator user)*

Part C: Static Imaging and Verification (Windows)

1. Access your Windows forensic VM "WINFOR01" from your Workspace.



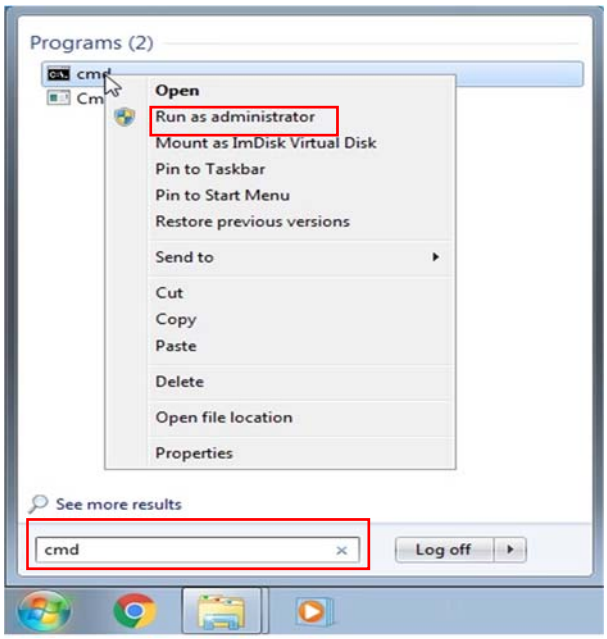
2. Locate the flash drive image in the under the Lab Resources folder placed on the Desktop.



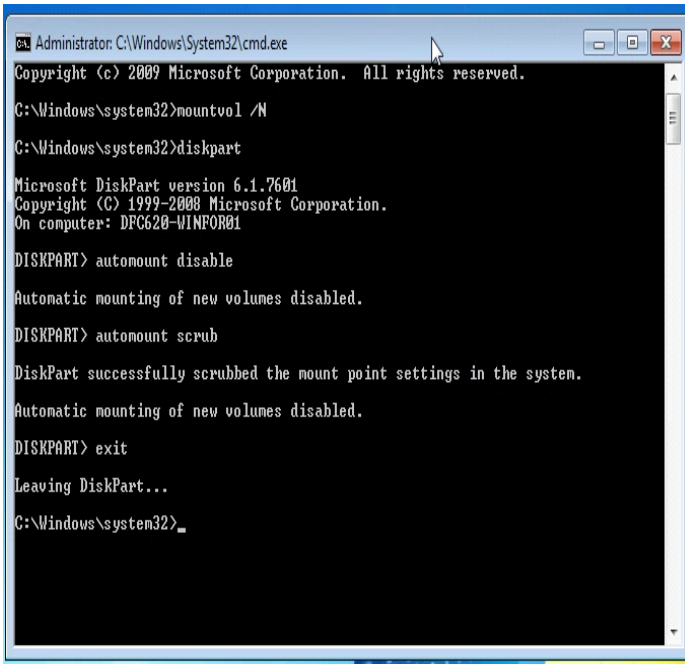
- (*We will be mounting the "FlashDrive" image file instead of plugging in a physical flash drive as one would do in practice.*

3. Lunch the command prompt as an administrator.

- From the Start Menu, type “cmd” in the search box.
- From the search results, run the “cmd” application as an administrator.

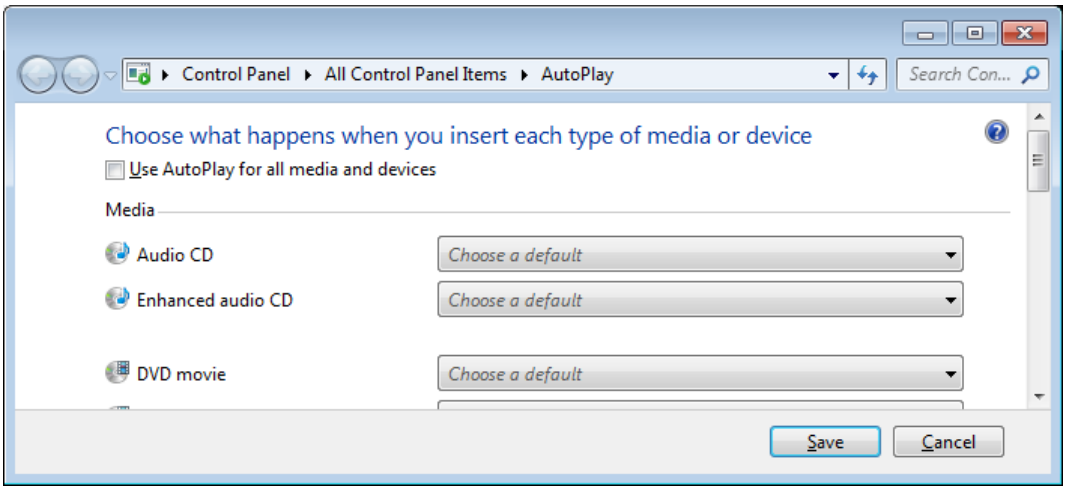


4. Disable auto-mounting: type the following commands at an Administrator command prompt:



- admin> mountvol /N
- or use the DISKPART utility:
  - admin> diskpart
  - DISKPART> automount disable
  - Automatic mounting of new volumes disabled.
  - DISKPART> automount scrub
  - DiskPart successfully scrubbed the mount point settings in the system.
  - Automatic mounting of new volumes disabled.
  - DISKPART> exit
  - admin> exit

5. Turn off AutoPlay in the Control Panel:



6. In practice, we would also use a hardware write blocker between the forensic workstation and the universal serial bus (USB) media, but this is a virtual lab so we do not have physical elements.

   IMPORTANT: If we were using a physical flash drive, At this point, we would insert the flash drive in a free USB port and confirm that the drive does not appear in Windows Explorer. Additionally, we would normally image the entire physical device without mounting the filesystem. However, for this exercise, we will be mounting and image of a flash drive; we will be imaging a partition of the mounted drive that represents our evidence USB flash device. Therefore, in the steps that follow, we will re-enable auto-mounting, mount the provided flash drive Image so that we can access just that particular partition.

7. Type the following at an Administrator command prompt:

   admin> mountvol /Y

   or use the DISKPART utility:

   admin> diskpart

   DISKPART> automount enable

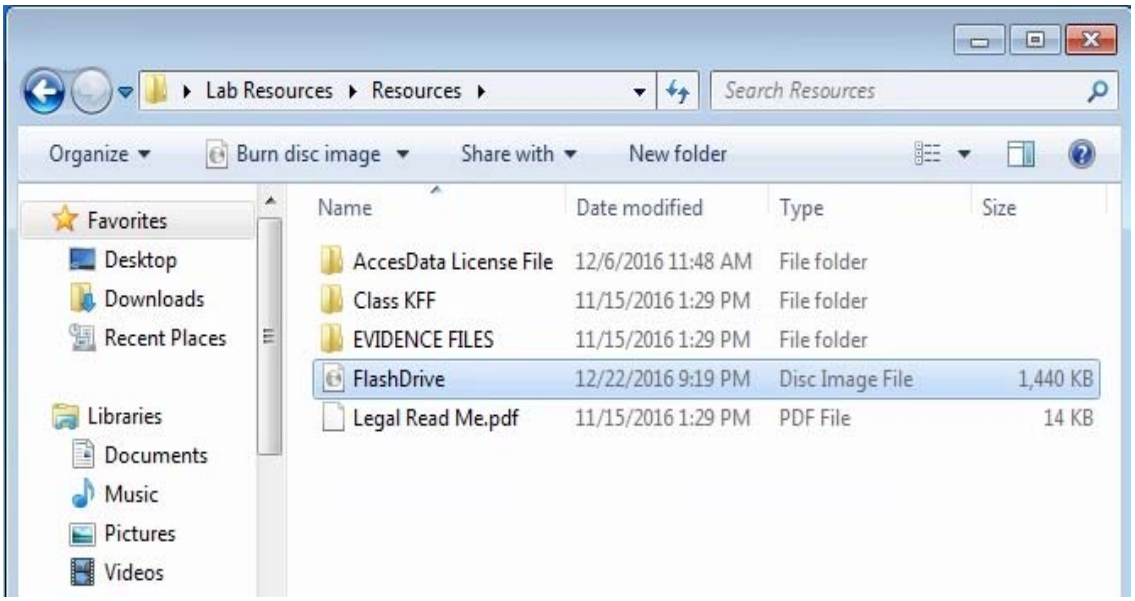
   Automatic mounting of new volumes enabled.

   DISKPART> exit

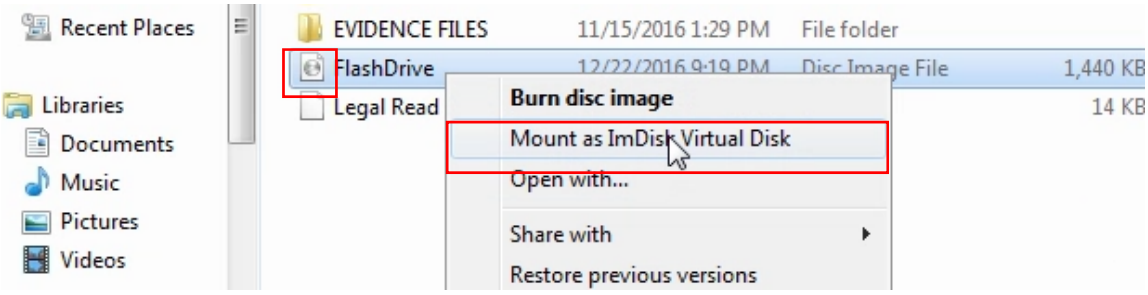
   admin> exit

8. Let's mount the flash drive image (This is equivalent to inserting the USB stick in a USB port).

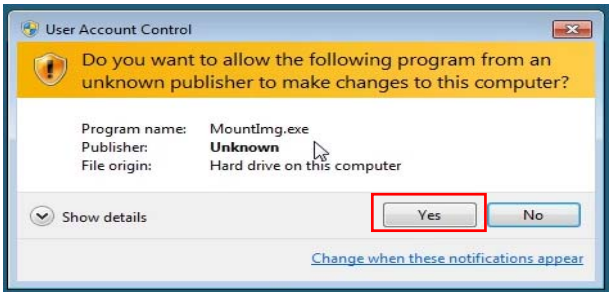
   a. Navigate to the flash location of the flash drive image under ~Desktop >Lab resources > Resources as depicted below.



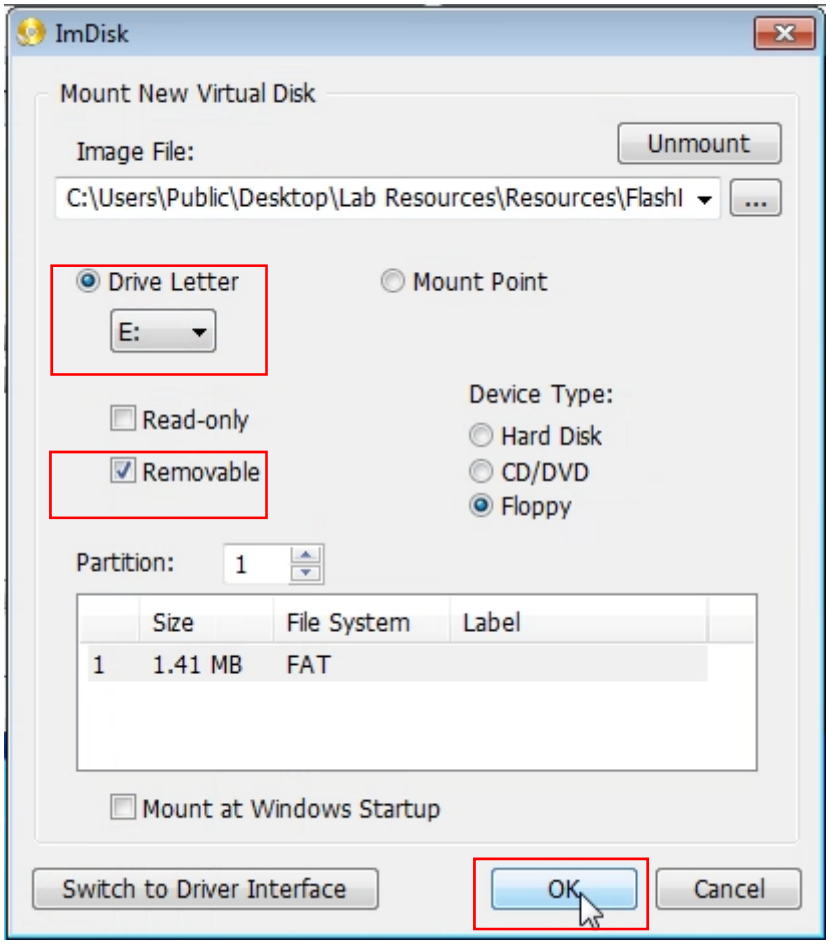
   b. Mount the "FlashDrive" image file as a virtual Disk as depicted below by right mouse clicking (or Ctrl Clicking for Mac users) on the icon of the flash drive image file and selecting "Mount as ImDisk Virtual Disk" from the Menu.



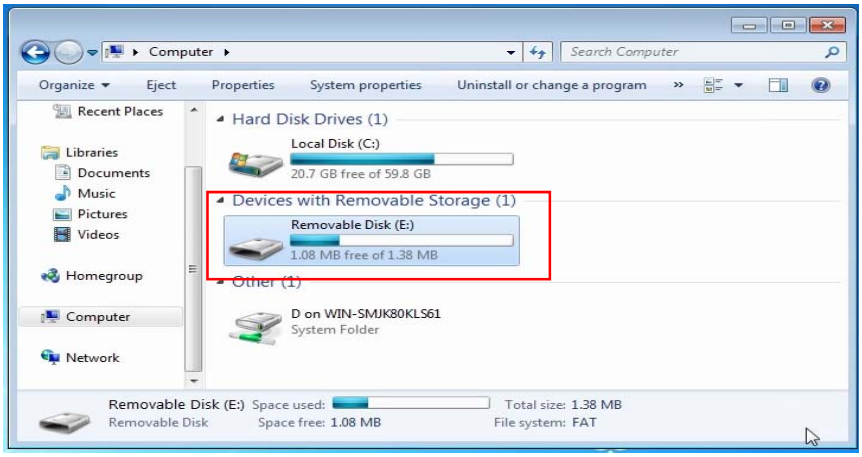
   c. When presented with the User Account control warning below, click yes to continue.



d. Select the drive letter for the virtual drive that we are mounting, select the "Removable" option and click OK to continue.

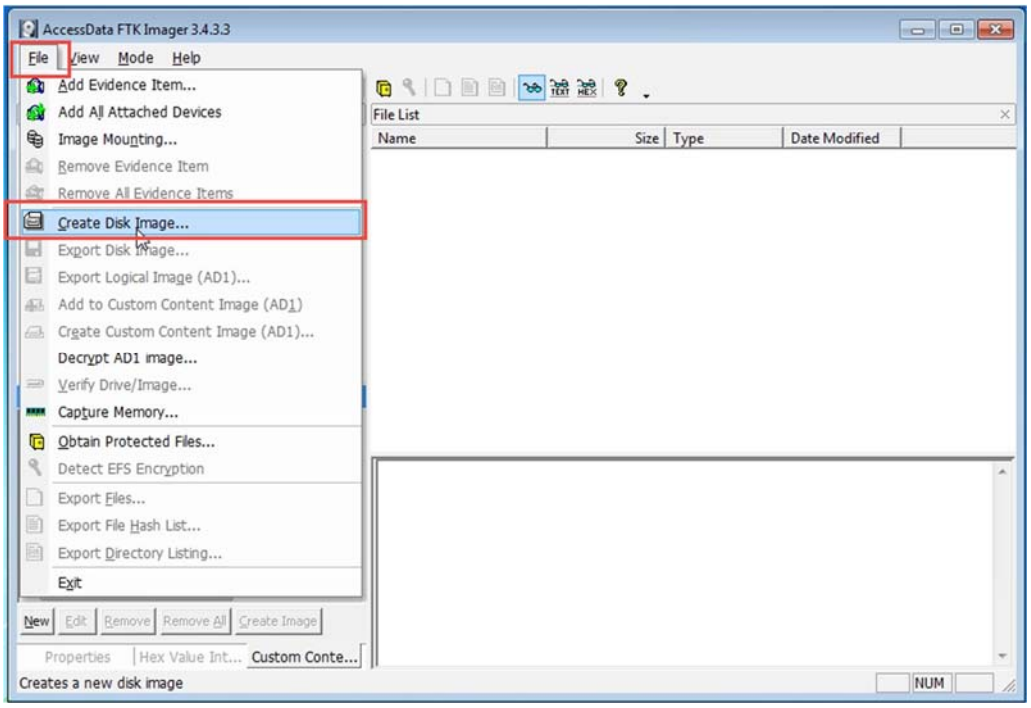


e. Verify that the drive is mounted and appearing under the removable storage devices in "Computer".

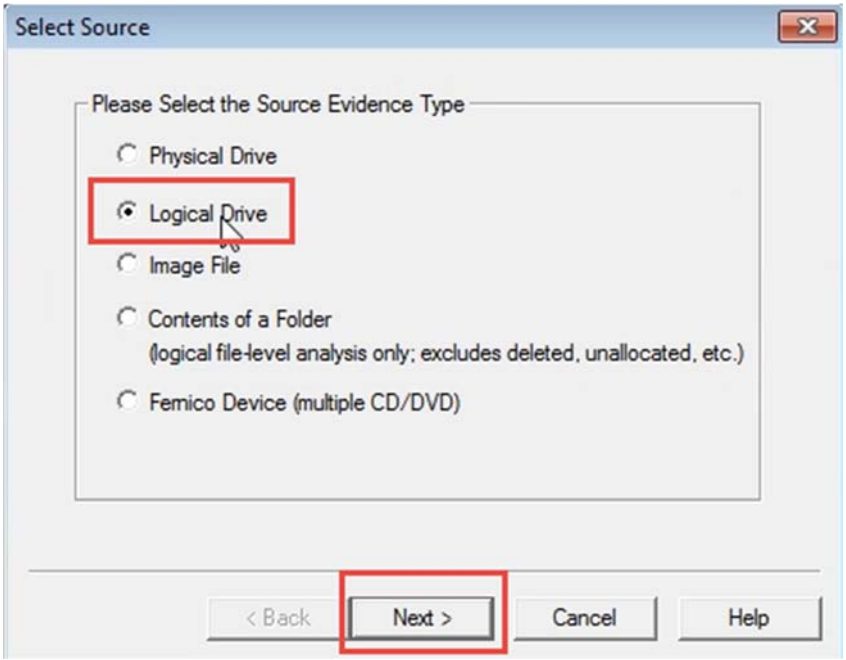


9. Create a forensic copy of the evidence partition of the flash drive:

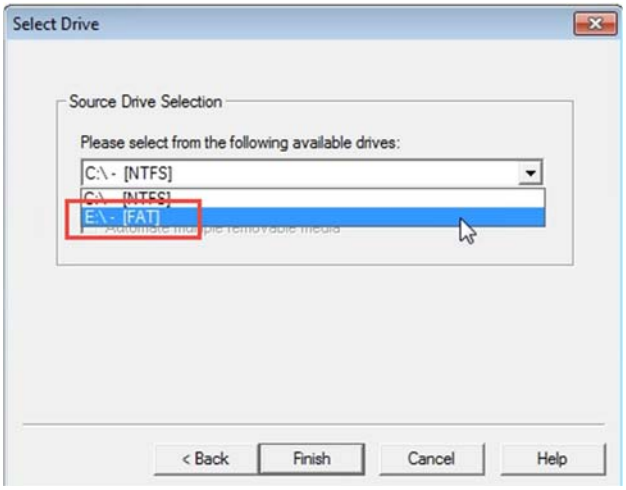
   a. Run FTK Imager; select File: Create Disk Image.



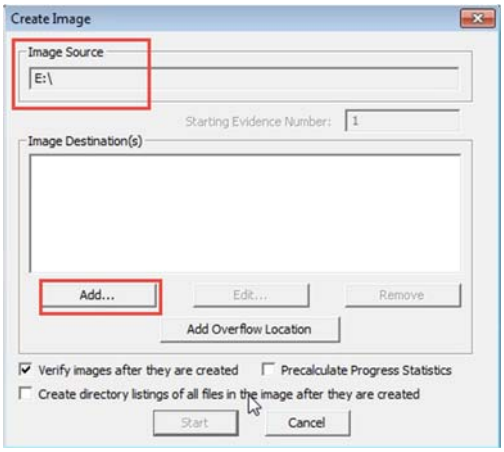
   b. Choose Logical Drive, then Next.



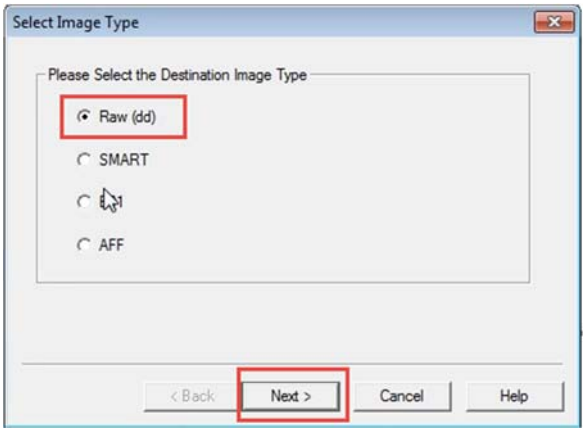
c. Choose the drive letter assigned to your USB stick, then Finish.



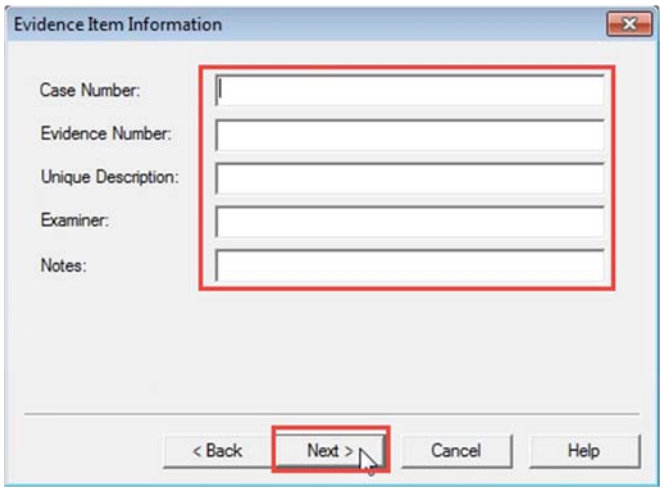
d. Check "Verify images after they are created" and click Add.



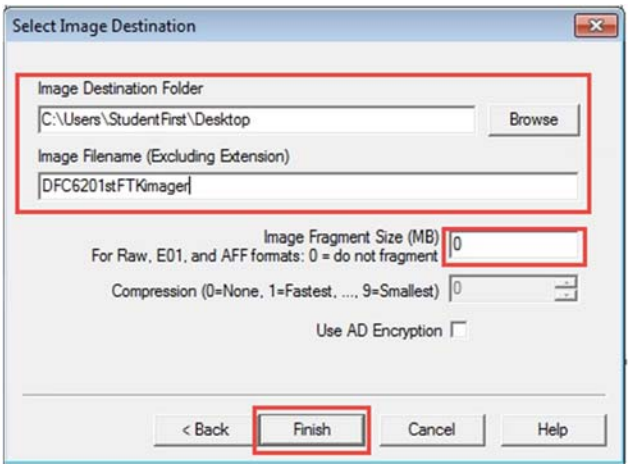
e. Select "Raw (dd)" then Next.



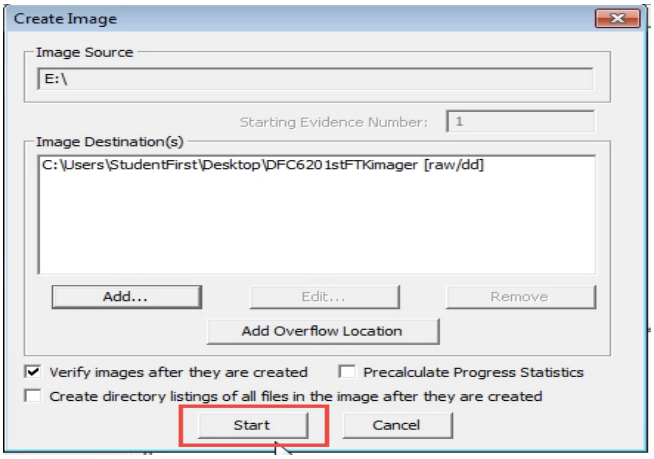
f. Complete the fields on this screen then click “Next”.



g. Select a destination for your image (on your computer, not on the flash drive), enter a filename, set Image Fragment Size to 0, and then select Finish.

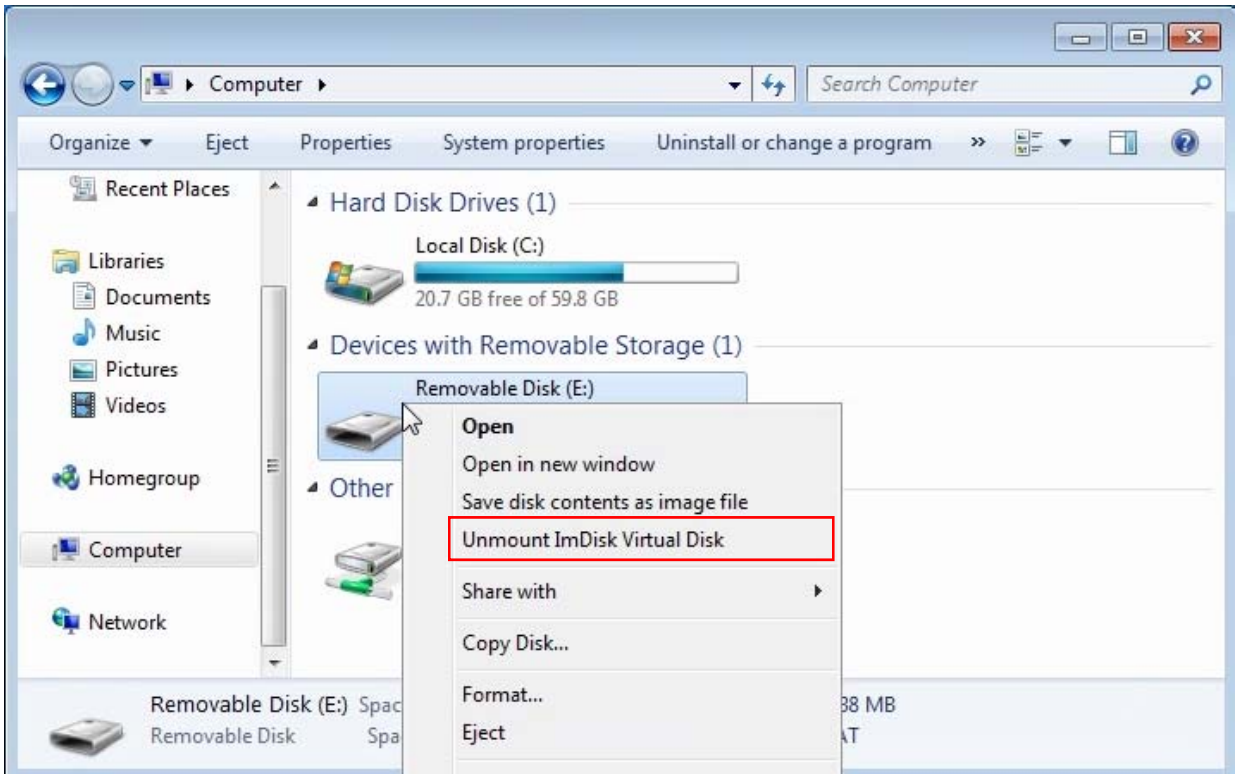


h. Click Start on the next screen and wait for the image creation to complete.



10. The image hash value will be displayed when the image completes, or you can compute the hash value of the image you just created (right click on the image file in Forensics Toolkit (FTK), then select Verify Drive/Image).

11. Unmount the "Virtual Disk".



12. Complete your lab notes as well as your report for this Part C only. Complete the lab report and lab notes using the templates provided. Your lab notes must include dates and times as well as specific descriptions of what you did and the results.